Regulamento para certificação de Sistemas de Gestão de Segurança da Informação

Válido a partir de 14.11.2016
(logomarca atualizada em 01.03.18)

RINA
Via Corsica 12
16128 Genova - Italia

tel +39 010 53851
fax +39 010 5351000
web site : www.rina.org

Regulamentos Técnicos

CONTEÚDO

CAPÍTULO 1
GERAL

1.1

Esse Regulamento define os procedimentos adicionais e/ ou substitutivos aplicados pelo RINA para a certificação dos Sistemas de Gestão da Segurança alimentar em relação ao que já foi definido no

Regulamento Geral para Certificação de Sistemas de Gestão

Os parágrafos desse Regulamento se referem aos (e mantém o mesmo número de) parágrafos correspondentes no Regulamento Geral para a Certificação de Sistemas de Gestão para o qual mudanças e/ ou adições foram realizadas.

1.2

Mudança em relação do Regulamento Geral:

"RINA realiza a certificação de acordo com os requisitos da ISO/IEC 17021:2015 e ISO/IEC 27006:2015 das organizações para as quais o Sistema de Gestão . . . ."

1.7

Adição ao Regulamento Geral:

A terminologia usada nesse regulamento é também indicada na ISO/IEC 27001:2013.

CAPÍTULO 3
CERTIFICAÇÃO INICIAL

3.1

Adição ao Regulamento Geral:

As organizações que desejam obter a certificação para seu Sistema de Gestão de de Segurança da Informação também devem fornecer ao RINA seus dados principais de organização / produção e localização das intalações, preenchendo todas as partes do formulário "Questionário Informativo" e o "Anexo ao Questionário Informativo para ISO / IEC". 27001 (Certificação ISMS) "disponível em www.rina.org e enviando-a para o RINA, que a utilizará para preparar uma cotação.

Em particular, a organização deve também informar ao RINA

Se o Sistema de gestão de segurança da informação incluir documentação (procedimentos, registros etc.) classificada como "confidencial" e / ou, em qualquer caso, não disponível para fins de certificação. O RINA avaliará se as condições são adequadas para continuar o processo de certificação.

CAPÍTULO 6
EXECUÇÃO DE AUDITORIAS

6.2.1

Adição ao Regulamento Geral:

O objetivo do estágio 1 também é:

- verificar se a avaliação de riscos, o plano para lidar com os riscos e a declaração de aplicabilidade (e quaisquer exclusões declaradas) são adequados em relação ao escopo de aplicação e atividades da organização
- verificar se as atividades terceirizadas foram adequadamente identificadas e monitoradas, confirmando, se necessário, a necessidade de realizar uma auditoria em terceiros

O estágio 1 é geralmente realizado nas instalações do cliente, de preferência em sua sede ou, em qualquer caso, em um local incluído no escopo da certificação e onde a auditoria do estágio 2 será realizada. Pode-se prever que, em casos específicos, avaliados caso a caso pelo RINA, parte da fase 1 não precise ser realizada nas instalações da organização

CAPÍTULO 7
GESTÃO DOS CERTIFICADOS DE CONFORMIDADE

7.1

Adição ao Regulamento Geral:

Os certificados emitidos fazem referência à declaração de aplicabilidade, sua edição e data de emissão, em vigor durante as auditorias realizadas nas instalações da organização

CAPÍTULO 9
REQUISITOS ESPECIAIS PARA ORGANIZAÇÕES MULTI-SITE

9.1

Adição ao Regulamento Geral:

Pelo menos as seguintes atividades também devem ser gerenciadas pela função central da organização:

- definição e gerenciamento da política de segurança
- avaliação, análise e tratamento de riscos
- definição e gerenciamento de controles

- definição e gerenciamento da declaração de aplicabilidade
- avaliação dos requisitos de treinamento

9.2

Adição ao Regulamento Geral:

"Se a organização observar os requisitos anteriores, o RINA sempre verificará a viabilidade da amostragem em todos os locais e poderá decidir se deve limitar essa amostragem na presença de:

- os resultados das auditorias internas da matriz e das unidades ou de auditorias de certificação anteriores;
- complexidade do Sistema de gestão de segurança da informação;
- complexidade dos sistemas de TI nas várias instalações;
- interação potencial com sistemas críticos de TI ou com sistemas de TI que gerenciam informações confidenciais;
- avaliação de risco.

CAPÍTULO 10
TRANSFERÊNCIA DE CERTIFICADOS ACREDITADOS

10.1

Adição ao Regulamento geral:

A organização, se aceitar a oferta econômica, deve enviar ao RINA a "solicitação de certificação" juntamente com os seguintes documentos:

- cópia controlada da declaração de aplicabilidade referenciada no certificado.

Regulamento para certificação de Sistemas de Gestão de Segurança da Informação

Publicação: RC/C 56

Edição Português

RINA
Via Corsica 12
16128 Genova - Italia

tel +39 010 53851
fax +39 010 5351000
web site : www.rina.org

Regulamento Técnico